

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-255005

(43)公開日 平成10年(1998) 9月25日

(51)Int.Cl.⁹

識別記号

F I

G 0 6 K 17/00

G 0 6 K 17/00

T

B 4 2 D 15/10

5 0 1

B 4 2 D 15/10

5 0 1 L

G 0 6 F 15/00

3 3 0

G 0 6 F 15/00

3 3 0 E

3 3 0 G

G 0 6 K 19/10

G 0 6 K 19/00

R

審査請求 有 請求項の数 6 O L (全 5 頁) 最終頁に続く

(21)出願番号

特願平9-58813

(22)出願日

平成9年(1997) 3月13日

(71)出願人 000164449

九州日本電気ソフトウェア株式会社

福岡市早良区百道浜2丁目4-1 NEC

九州システムセンター

(72)発明者 小島 弘士

福岡県福岡市早良区百道浜2-4-1 九

州日本電気ソフトウェア株式会社内

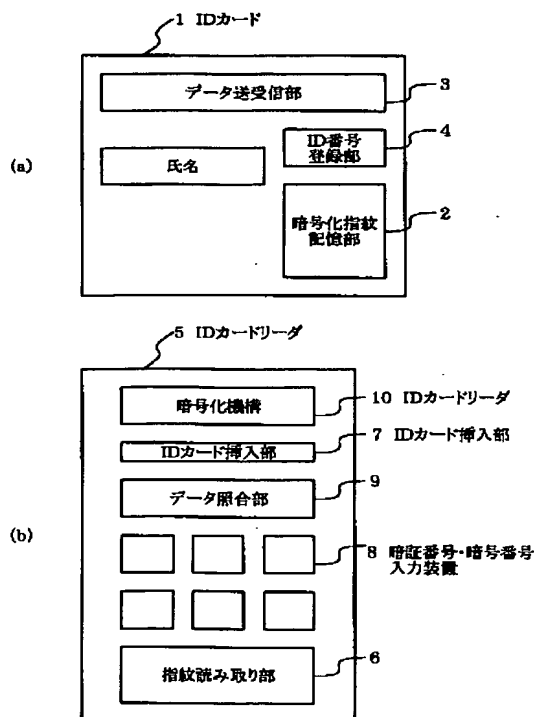
(74)代理人 弁理士 京本 直樹 (外2名)

(54)【発明の名称】 利用者認証方式

(57)【要約】

【課題】 IDカードの改ざんを防止する。

【解決手段】 暗号化指紋記憶部2には、本人の指紋が予め暗号化されて記憶されている。データ送受信部3は、ID番号登録部4に登録されているID番号と、暗号化指紋記憶部2に記憶されている暗号化されている指紋情報を、IDカードリーダ5へ送信する。指紋読み取り部6は、利用者の指紋を入力する。IDカード挿入部7は、IDカード1が入力されると、ID番号と暗号化されている指紋情報を受信する。暗証番号・暗号番号入力装置8は、照合部9で暗証番号照合時の暗証番号入力と、同じく照合部9で暗号化指紋情報照合時の暗号化番号入力とを行う。暗号化機構10は、指紋読み取り部6で読み取った指紋を、暗証番号・暗号番号入力装置8から入力された暗号番号に基づいて暗号化する。照合部9は、暗証番号照合と暗号化指紋情報照合で正しい結果が得られれば、セキュリティを解除する。



【特許請求の範囲】

【請求項1】 IDカードを利用した認証システムにおける利用者認証方式において、該IDカードを読み込むIDカードリーダは、入力された利用者の個人情報を該利用者によって指定された暗号化方法により暗号化し、暗号化された該個人情報と前記IDカードに予め格納されている個人情報とを比較することにより前記利用者を認証することを特徴とし、該IDカード内の該固有情報の改ざんを防止し該IDカード利用による認証システムのセキュリティを向上させる利用者認証方式。

【請求項2】 前記IDカードに格納されている個人情報は予め暗号化されていることを特徴とする請求項1記載の利用者認証方式。

【請求項3】 前記個人情報が、指紋情報であることを特徴とする請求項1記載の利用者認証方式。

【請求項4】 前記個人情報が、音声情報であることを特徴とする請求項1記載の利用者認証方式。

【請求項5】 前記個人情報が、眼情報であることを特徴とする請求項1記載の利用者認証方式。

【請求項6】 前記暗号化方法は前記IDカード内に複数用意され、前記利用者は暗号化番号を入力することにより該暗号化方法を指定することを特徴とする請求項1記載の利用者認証方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、利用者認証方式に関する。

【0002】

【従来の技術】従来、現金自動支払機などでは、利用者を認証するために、IDカードを入力させ、IDカードに予め磁気的に記録されている暗証番号と、利用者によりキーボードから入力された暗証番号とを照合するようにしている。しかし、この方法では、他人が不正に入手したIDカードから暗証番号を読み取り、不正に使用する場合があるため、新しい利用者認証方式、例えば公開特許公報；特開平4-342066「利用者認証方式」に記載されているように、IDカードに利用者の固有情報（例えば指紋）を記憶させておき、利用者認証時には、利用者から入力された固有情報とIDカードに記憶されている利用者の固有情報とを照合する方式が開発されている。

【0003】

【発明が解決しようとする課題】しかしながら、上述した公報の方法では、技術革新の激しい現代にあつては、暗証番号の場合と同様、IDカード内の固有情報が何らかの方法で改ざんされ、不正使用される可能性を有している。

【発明の目的】本発明の目的は、IDカードを利用した認証システムにおいて、IDカード内の固有情報を利用者しか知らない暗号化方法により暗号化することによ

り、IDカード内の固有情報の改ざんを防止し、IDカード利用による認証システムのセキュリティを確保する利用者認証方式を提供することにある。

【0004】

【課題を解決するための手段】第1の発明は、IDカードを利用した認証システムにおける利用者認証方式において、該IDカードを読み込むIDカードリーダは、入力された利用者の個人情報を該利用者によって指定された暗号化方法により暗号化し、暗号化された該個人情報と前記IDカードに予め格納されている個人情報とを比較することにより前記利用者を認証することを特徴とする。

【0005】また、第2の発明は、第1の発明における前記IDカードに格納されている個人情報は予め暗号化されていることを特徴とする。

【0006】さらに、第3の発明は、第1の発明における前記個人情報が、指紋情報であることを特徴とする。

【0007】さらに、第4の発明は、第1の発明における前記個人情報が、音声情報であることを特徴とする。

【0008】さらに、第5の発明は、第1の発明における前記個人情報が、眼情報であることを特徴とする。

【0009】さらに、第6の発明は、第1の発明における前記暗号化方法は前記IDカード内に複数用意され、前記利用者は暗号化番号を入力することにより該暗号化方法を指定することを特徴とする。

【0010】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して詳細に説明する。

【0011】図1は、本発明の一実施形態を示すブロック図であり、(a)は、IDカードの構成図、(b)は、IDカードリーダの構成図である。また、図2は本発明の動作フローチャートである。

【0012】図1(a)に掲載しているとおり、IDカード1は、暗号化指紋記憶部2、データ送受信部3、ID番号登録部4から構成され、また図1(b)に掲載しているとおり、IDカードリーダ5は、指紋読み取り部6、IDカード挿入部7、暗証番号・暗号番号入力装置8、照合部9、暗号化機構10から構成されている。

【0013】図1(a)において、暗号化指紋記憶部2には、本人の指紋が予め暗号化されて記憶されている。ここで、暗号化の種類はシステムで複数用意されており、そのうちの1つで暗号化した後は、本人はその暗号化番号を、暗証番号とともに記憶しておく必要がある。また、指紋の暗号化技術は、周知であるため、ここでは記述していない。データ送受信部3は、IDカード1がIDカードリーダ5に入力されると、ID番号登録部4に登録されているID番号と、暗号化指紋記憶部2に記憶されている暗号化されている指紋情報を、IDカードリーダ5へ送信する。

【0014】図1(b)において、指紋読み取り部6

は、利用者の指紋を入力する場所である。IDカード挿入部7には、データ送受信機能を具備しており、IDカード1が入力されると、データ送受信部3からID番号と暗号化されている指紋情報を受信する。暗証番号・暗号番号入力装置8は、照合部9で暗証番号照合時の暗証番号入力と、同じく照合部9で暗号化指紋情報照合時の暗号化番号入力とを行う場所である。暗号化機構10は、指紋読み取り部6で読み取った指紋を、暗証番号・暗号番号入力装置8から入力された暗号番号に基づいて暗号化する部分である。照合部9は、暗証番号照合と暗号化指紋情報照合で正しい結果が得られれば、この利用者が本人であると認証し、セキュリティを解除する。

【0015】(動作の説明)次に、本発明の特徴部分の動作について図1、2を参照して詳細に説明する。

【0016】認証者がIDカード1をIDカードリーダー5に挿入すると、ID番号登録部4に登録されているID番号と、暗号化指紋記憶部2に記憶されている暗号化されている指紋情報をデータ送受信部3よりIDカードリーダー5へ送信する(ステップA)。

【0017】IDカードリーダー5では、IDカード挿入部7で、ID番号と暗号化指紋情報を受信すると、利用者に対して暗証番号・暗号番号入力装置8から暗証番号の入力を促す。利用者が暗証番号を入力すると、あらかじめ登録されているID番号及び暗証番号と、カードから受信したID番号及び利用者が入力した暗証番号とを照合し、正しければ次に暗証番号・暗号番号入力装置8からの暗号番号の入力及び指紋読み取り部6からの指紋の入力を促す(ステップB)。

【0018】利用者が暗号番号と指紋を入力すると、暗号化機構10は、入力された暗号番号に相当する暗号化ツール(図示していないが、予め具備しているものとする)を用いて入力された指紋を暗号化し、暗号化指紋情

報を作成する。照合部9は、作成された暗号化指紋情報と、IDカード1から受信した暗号化指紋情報とを照合し、正しければ当該システムのセキュリティを解除する(ステップC)。

【0019】尚、本実施例では、指紋情報を用いたが、音声情報、眼情報その他の個人を特定できる情報であれば何でも良い。

【0020】

【発明の効果】以上説明したように、本発明は、入力された利用者の個人情報を該利用者によって指定された暗号化方法により暗号化し、暗号化された該個人情報とIDカードに予め格納されている個人情報とを比較して利用者を認証するようにしたことにより、IDカード内の固有情報の改ざんを防止し、IDカード利用による認証システムのセキュリティを向上させる効果がある。

【図面の簡単な説明】

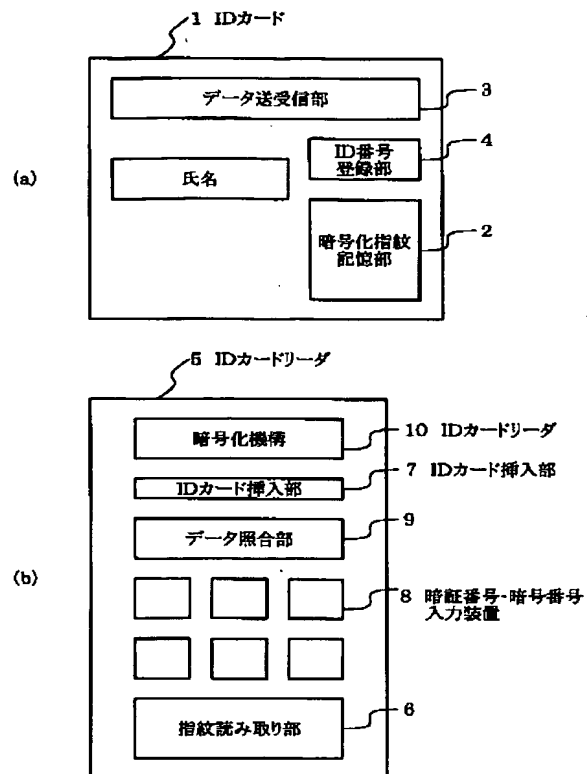
【図1】(a)は、本発明のIDカードの一実施例を示す構成図、(b)は、本発明のIDカードリーダーの一実施例を示す構成図である。

【図2】本発明の動作を示すフローチャートである。

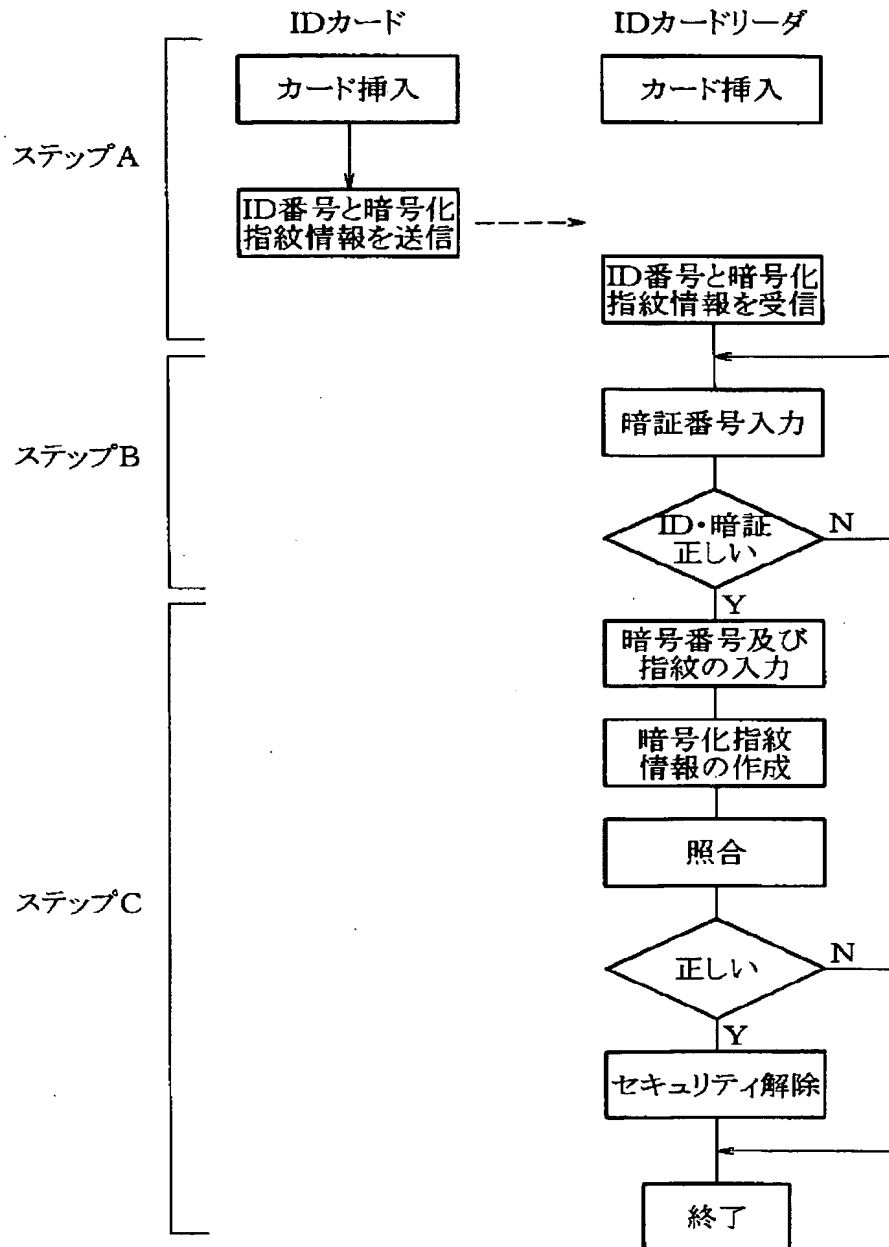
【符号の説明】

- | | |
|----|---------------|
| 1 | IDカード |
| 2 | 暗号化指紋記憶部 |
| 3 | データ送受信部 |
| 4 | ID番号登録部 |
| 5 | IDカードリーダー |
| 6 | 指紋読み取り部 |
| 7 | IDカード挿入部 |
| 8 | 暗証番号・暗号番号入力装置 |
| 9 | データ照合部 |
| 10 | 暗号化機構 |

【図1】



【図2】



フロントページの続き

(51)Int.Cl.⁶

G 0 7 F 7/12

識別記号

F I

G 0 7 F 7/08

B